



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/837,283	04/18/2001	Paul H. Feinberg	SONY 3.0-029	9632
530	7590	03/10/2006	EXAMINER	
LERNER, DAVID, LITTENBERG, KRUMHOLZ & MENTLIK 600 SOUTH AVENUE WEST WESTFIELD, NJ 07090			TRUONG, THANHNGA B	
			ART UNIT	PAPER NUMBER
			2135	

DATE MAILED: 03/10/2006

Please find below and/or attached an Office communication concerning this application or proceeding.



UNITED STATES PATENT AND TRADEMARK OFFICE

---

Commissioner for Patents  
United States Patent and Trademark Office  
P.O. Box 1450  
Alexandria, VA 22313-1450  
[www.uspto.gov](http://www.uspto.gov)

**MAILED**

MAR 10 2006

Technology Center 2100

**BEFORE THE BOARD OF PATENT APPEALS  
AND INTERFERENCES**

Application Number: 09/837,283  
Filing Date: April 18, 2001  
Appellant(s): FEINBERG, PAUL H.

---

Mayush Singhvi  
For Appellant

**EXAMINER'S ANSWER**

This is in response to the appeal brief filed December 27, 2005 appealing from the Office action mailed May 19, 2005.

**(1) Real Party in Interest**

The statement identifying the real party in interest is contained in the brief.

**(2) Related Appeals and Interferences**

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

**(3) Status of Claims**

The statement of the status of claims contained in the brief is correct. The changes are as follows:

Claims 1-5, 8-9, 12-17, 21-24, 27-33 are pending for rejection. Claims 6-7, 10-11, 18-20, 25-26 are objected.

**(4) Status of Amendments After Final**

No amendment after final has been filed.

**(5) Summary of Claimed Subject Matter**

The summary of claimed subject matter contained in the brief is correct.

**(6) Grounds of Rejection to be Reviewed on Appeal**

The appellant's statement of the grounds of rejection to be reviewed on appeal is substantially correct. The changes are as follows:

Claims 8-9, 12-16, 23-24, 27-31 are rejected under 35 U.S.C. 102(b) as being anticipated by Takagi et al (US 5,109,152).

Ohno (US 5,355,413) is being withdrawn by the Examiner for the rejection of claims 8 and 23.

Claims 1-5 are rejected under 35 U.S.C. 103(a) as being unpatentable over Takagi et al (US 5,109,152).

Claims 17, 21-22, 32-33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Takagi et al (US 5,109,152), and further in view of Nakagawa et al (US 5,651,123).

**(7) Claims Appendix**

The copy of the appealed claims contained in the Appendix to the brief is correct.

**(8) Evidence Relied Upon**

No evidence is relied upon by the examiner in the rejection of the claims under appeal.

**(9) Grounds of Rejection**

The following ground(s) of rejection are applicable to the appealed claims:

Claims 8-9, 12-16, 23-24, 27-31 are rejected under 35 U.S.C. 102(b) as being anticipated by Takagi et al (US 5,109,152).

a. Referring to claim 8:

i. Takagi teaches:

(1) receiving a first value (or data) from the device, the first value being different from an identifier associated with the device; determining the identifier from the value, the value being a function of the identifier and the number of times the device has been authenticated; comparing the identifier determined from the value against a pre-stored identifier; authenticating the device based on the result of the comparison [i.e., the procedure of creating the identifier described above in connection with Figure 6 is completely identical to the procedure of data encryption shown in Figure 5, and it is possible to have the identifier creation process and data encryption process concurrently. Namely, the output of the encryption processes 223-226 in Figure 6 is sent to the second device 202 as an output (encrypted output of transmission data) of the encryption means 204. Specifically, the output of the encryption process 226, i.e., the identifier 231, in Figure 6 is the output of the encryption means 204 for the fixed pattern (P) 215 in Figure 5, and it is stored in the second register 208. Next, the second device 202 uses the second encryption means 211 which performs the same operation as of the first encryption means 204, third register 212 and third exclusive-OR operation means 213 to create comparison data in the same procedure as that of the first device 201 for creating the identifier 231. The comparison data is stored in the third register 212. Finally, the second device 202 uses the comparison means 214 to compare the identifier 231 stored in the second register 208 with the comparison data stored in the third register 212 thereby to verify whether or

Art Unit: 2135

not the communication data has been tampered (column 12, line 59 through column 13, line 40). In addition, Similarly, in the second comparison means 156, the result of comparison between the random number data S.sub.2 which is inferred to have been produced by the transaction IC card 150 and the random number data S.sub.0 which has been actually generated by the second random number generation means 151 becomes a second control signal C.sub.2 for the second processing means 160, and only if both data match, it grants the second processing means 160 to have the information exchange (column 10, lines 31-40)].

b. Referring to claims 9, 12-14:

i. These claims have limitations that is similar to those of claim 8, thus they are rejected with the same rationale applied against claim 8 above.

c. Referring to claim 15:

i. This claim has limitations that is similar to those of claim 3, thus it is rejected with the same rationale applied against claim 3 above.

d. Referring to claim 16:

i. Takagi further teaches:

(1) wherein the function is intended to make it difficult to predict the next value to be received [i.e., (1) the identifier is dependent on all bits of data of the plain text block. (2) For a plain text m, identifier creation means f, and identifier  $a=f(m)$ , it is very difficult to obtain x which meets the following:  $f(m)=f(x)$  (column 12, lines 51-57)].

e. Referring to claim 23:

i. Takagi teaches:

(1) maintaining a seed value which is equivalent to a seed value maintained at the source, the seed changing over time, generating a value based on the seed and based on a value identifying the destination whereby the generated value is different from the seed and the destination's identification value; transmitting the generated value to the source; and [i.e., referring to Figure 5, as the initial state, a same value l is stored in the first, second and third registers 205,

Art Unit: 2135

208 and 212. For the I, a random number shared confidentially by the first and second communication devices (column 11, lines 41-44). Initially, when the transaction IC card 150 is inserted in the card terminal 100 which is equipped with the confirmation IC card 110, the first random number generation means 111 in the confirmation IC card 110 generates random number data R.sub.0, and the first encryption means 112 encrypts the random number data R.sub.0 provided by the first random number generation means 111 by using the first encryption key KE.sub.1 which is stored in advance in the confirmation IC card 110, and sends it to the transaction IC card 150 (column 9, lines 33-42)];

(2) being authenticated to receive information from the source or send information which will be used by the source, the authentication being dependant upon the source using the seed to extract the destination's identification value and comparing the destination's identification value with the value of a destination known by the source to be authentic **[this limitation is similar to those of claim 8, thus it is rejected with the same rationale applied against claim 8 above]**.

f. Referring to claims 24, 27-29:

i. These claims have limitations that is similar to those of claims 2-3, thus they are rejected with the same rationale applied against claims 2-3 above.

g. Referring to claim 30:

i. This claim has limitations that is similar to those of claim 23, thus it is rejected with the same rationale applied against claim 23 above.

h. Referring to claim 31:

i. This claim has limitations that is similar to those of claim 8, thus it is rejected with the same rationale applied against claim 8 above.

Claims 1-5 are rejected under 35 U.S.C. 103(a) as being unpatentable over Takagi et al (US 5,109,152).

a. Referring to claim 1:

i. Takagi teaches:

(1) providing a first device having a first identifier; providing a second device having a second identifier [i.e., the first communication device is provided with random number generation means and first encryption means, and the second communication device is provided with second encryption means, and therefore a random number flowing from the first communication device to the second communication device is encrypted by the first encryption means, and a random number flowing from the second communication device to the first communication device is encrypted by the second encryption means (column 4, lines 46-57)];

(2) the first device sending the first identifier to the second device during a first connection [i.e., the first processing means which has been granted the information exchange sends the transmission data to the first communication means, and the first communication means 1 uses the random number data provided by the random number generation means to encrypt the entered transmission data and sends it to the card terminal. The encrypted data received by the card terminal is entered to the second communication means, and the second communication means uses the random number data received from the IC card to decrypt the entered encrypted data and enters it to the second processing means, which is the second communication device (column 4, lines 11-23)];

(3) the second device sending the second identifier to the first device during the first connection [i.e., the second processing means sends the transmission data to the second communication means, and the second communication means uses the random number data received from the IC card to encrypt the entered data and sends it to the IC card. The encrypted data received by the IC card is entered to the first communication means, and the first communication means uses the random number data provided by the random number generation means to decrypt the entered encrypted data and enters it to the first processing means (column 4, lines 24-36)];

(4) the first device storing the second identifier and the second device storing the first identifier; when the first and second devices are disconnected and reconnected, the first device sending the first identifier to the second device and the second device sending the second identifier to the first device during the first reconnection, and each device comparing the received identifier against the stored identifier and sending additional information to the other device depending upon the result of the comparison [i.e., the procedure of creating the identifier described above in connection with Figure 6 is completely identical to the procedure of data encryption shown in Figure 5, and it is possible to have the identifier creation process and data encryption process concurrently. Namely, the output of the encryption processes 223-226 in Figure 6 is sent to the second device 202 as an output (encrypted output of transmission data) of the encryption means 204. Specifically, the output of the encryption process 226, i.e., the identifier 231, in Figure 6 is the output of the encryption means 204 for the fixed pattern (P) 215 in Figure 5, and it is stored in the second register 208. Next, the second device 202 uses the second encryption means 211 which performs the same operation as of the first encryption means 204, third register 212 and third exclusive-OR operation means 213 to create comparison data in the same procedure as that of the first device 201 for creating the identifier 231. The comparison data is stored in the third register 212. Finally, the second device 202 uses the comparison means 214 to compare the identifier 231 stored in the second register 208 with the comparison data stored in the third register 212 thereby to verify whether or not the communication data has been tampered (column 12, line 59 through column 13, line 40)];

ii. Although, Takagi does not explicitly mention:

(1) disconnected and reconnected between the first and second devices.

iii. Examiner takes Official Notice that:

(1) the disconnection and reconnection between the first and second devices were well known at the time the invention was made.



iii. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:

(1) include the disconnection and reconnection between the first and second devices. Such an application would have been obvious because Takagi teaches applicability to insert the first device (i.e., IC card) in the card terminal, which is the second device, and because the execution of inserting, un-inserting, and re-inserting the IC card were well known.

b. Referring to claim 2:

i. Takagi further teaches:

(1) wherein the step of sending an identifier to the other device includes sending a value that is based on, but not equivalent to, the identifier [i.e., **next, a method of creating the identifier will be explained with reference to Figure 6. Figure 6 is an explanatory diagram showing the procedure of creating the identifier, in which 221 is a plain text block (M.sub.1, M.sub.2, M.sub.3), 215 is a fixed pattern (P) shown in Figure 5, 222 is an initial value I of the first register 205 (column 12, lines 29-34)].**

c. Referring to claim 3:

i. Takagi further teaches:

(1) wherein the value sent by the first device is based on the number of times the first device has connected to the second device [i.e., **accordingly, unless the transmission data is altered accidentally or intentionally, the first register 205 and second register 208 always stores the same value. By repeating the process of the leading n-bit data M.sub.1 for the M.sub.2 and M.sub.3 identically, the restored original data are stored sequentially in the restoration block storage means 210 (column 12, lines 15-21)].**

d. Referring to claim 4:

i. Takagi further teaches:

(1) wherein the difference between the different values sent each time is pseudo-random [i.e. **the following explains this embodiment with reference to Figure 5. As the initial state, a same value I is stored in the first,**

second and third registers 205, 208 and 212. For the I, a random number shared confidentially by the first and second communication devices in the first through third embodiments can be used, for example (column 11, lines 40-45)].

e. Referring to claim 5:

i. Takagi further teaches:

(1) wherein the value sent by the first device is determined based on at least one mathematical operation, and at least one of the purposes of the mathematical operation is to make it difficult to predict the next value to be sent [i.e., (1) the identifier is dependent on all bits of data of the plain text block. (2) For a plain text  $m$ , identifier creation means  $f$ , and identifier  $a=f(m)$ , it is very difficult to obtain  $x$  which meets the following:  $f(m)=f(x)$  (column 12, lines 51-57)].

Claims 17, 21-22, 32-33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Takagi et al (US 5,109,152), and further in view of Nakagawa et al (US 5,651,123).

a. Referring to claim 17:

i. Takagi teaches:

(1) a pseudo-random number generator using the increment counter value as a seed; memory for storing a value identifying the device; instructions including using the value of the increment counter to extract the value identifying the device from a value transmitted from the device, comparing the identification value with the value stored in memory, and taking the action dependant upon the results of the comparison [i.e., referring to Figure 9, a card terminal 400 comprises a random number generation means 401 which generates a random number  $R$ , a first computation means 402 which performs a functional computation  $F_{sub.1}$  for first confidential data  $K_{sub.1}$  and the random number  $R$  provided by said random number generation means 401, comparison means 403 which compares data provided by said first computation means 402 and data entered from an IC card 450, first processing means 406 which performs such

Art Unit: 2135

**data processing as data input/output, storing and operation, first encryption means 404 which encrypts the data sent out from said first processing means by using a first encryption key KE.sub.1, second decryption means 405 which decrypts encrypted data entered from the IC card 450 by using a second decryption key KD.sub.2 (column 1, lines 17-31)];**

ii. However, Takagi does not explicitly mention:

(1) an increment counter associated with a value representing the number of times the system has taken an action in response to a signal from the device; instructions including using the value of the increment counter to extract the value identifying the device from a value transmitted from the device.

iii. Whereas, Nakagawa teaches:

(1) Figure 1 shows an example of a conventional program execution control device (hereinafter referred to as a "program control unit") for controlling a program execution order in a microprocessor or the like. With reference to FIG. 1, a conventional program control unit includes a program counter (PC) 300, an instruction memory 32, an instruction decoder 34, an incrementer 302 and a selector 304. Instruction memory 32 stores instructions of a program in the order of program addresses. Program addresses are ordinarily set to be incremented one by one. In instruction memory 32, the program addresses are arranged in a continuous memory space whose addresses are incremented one by one. Instruction memory 32 is for reading an instruction word 38 (of m-bit) from an applied n-bit address 310 and applying the word to instruction decoder 34 (column 1, lines 22-36). Nakagawa further discloses with reference to Figure 4, the program control unit of the present embodiment includes an instruction memory 32, an instruction decoder and a pseudo-random number program counter 30. Instruction memory 32 and instruction decoder 34 are the same as those of the conventional device shown in Figure 1, except that a program stored in instruction memory 32 is different from that of Figure 1. The program will be detailed later. An output 38 of instruction memory 32, a control signal 40, a select signal 42 and a jump address 44 output from instruction decoder 34 are also the same as those

Art Unit: 2135

shown in FIG. 1 and no detailed description thereof will be repeated here (**column 7, lines 12-24**).

iv. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:

(1) include a pseudo-random number program counter and an instruction memory (in Takagi) to improve the communication between the two devices.

v. The ordinary skilled person would have been motivated to:

(1) include a pseudo-random number program counter and an instruction memory (in Takagi) to provide program execution control devices for storing instructions in an instruction storage device and designating addresses of the device to read the instructions at high speed in a specific order and apply the same to a program execution device and a method thereof (**column 1, lines 8-12 of Nakagawa**).

b. Referring to claim 21:

i. This claim has limitations that is similar to those of claim 17, thus it is rejected with the same rationale applied against claim 17 above.

c. Referring to claim 22:

i. This claim has limitations that is similar to those of claim 17, thus it is rejected with the same rationale applied against claim 17 above.

d. Referring to claim 32:

i. This claim has limitations that is similar to those of claim 17, thus it is rejected with the same rationale applied against claim 17 above.

e. Referring to claim 33:

i. Takagi further teaches:

(1) wherein the second device further comprises a checksum algorithm providing a value indicative of whether the prestored value was erased [i.e., the procedure of verifying the identifier will be described with reference to Figure 5. First, a processing means (not shown) of the second device 202 replaces the last n-bit data out of the data stored in the restoration block storage means 210 with the fixed pattern 216. In case communication has

taken place normally, the original data to be replaced (that is “the prestored value was erased”) is equal to the fixed pattern 216 (column 13, lines 3-7)].

**(10) Response to Arguments**

I. Regarding to the Appellant’s arguments to claim 8 on anticipation by Takagi. Appellant states that “Takagi does not disclose using the “number of times the device has been authenticated” for a value used to determine the identifier. First of all, the claimed “**number of times the device has been authenticated**” that recites is read on by the prior art.

Takagi teaches in the first comparison means 116, the result of comparison between the random number data R.sub.2 which is inferred to have been produced by the confirmation IC card 110 and the random number data R.sub.0 which has been actually provided by the first random number generation means 111 becomes a first control signal C.sub.1 for the first processing means 120. If both data match, the first comparison means 116 grants the first processing means 120 to have the information exchange with the transaction IC card 150, or inhibits the information exchange if the data do not match. Similarly, in the second comparison means 156, the result of comparison between the random number data S.sub.2 which is inferred to have been produced by the transaction IC card 150 and the random number data S.sub.0 which has been actually generated by the second random number generation means 151 becomes a second control signal C.sub.2 for the second processing means 160, and only if both data match, it grants the second processing means 160 to have the information exchange. **This means the number of times the IC card has been authorized are unlimited as long as the inputted data matched the predetermined data the information exchange is allowed, otherwise there is no exchange of data** (column 10, lines 21-40 of Takagi). Thus, Takagi teaches the claimed “number of times the device has been authenticated”. In addition, Appellant has argued if the index value (number of times the device has been authenticate) is 1, then the pseudorandom number generator may obtain the first prime number after four (which is 5) ..... point which is 71 (see Appellant’s Appeal Brief, page 7, lines 7-12). This clarification/limitation is not addressed any where in the claim. In fact, appellant is trying

Art Unit: 2135

to equate the index value as being the same as **(number of times the device has been authenticate)**. This equating fact is unusual because it is irrelevant for an index value being interpreted as the **number of times the device has been authenticate**. In response to appellant's argument that the references fail to show certain features of appellant's invention, it is noted that the features upon which appellant relies (i.e., **if the index value is the number of times the device has been authenticate and equals to 1, then the pseudorandom number generator may obtain the first prime number after four (which is 5) ..... point which is 71**) are not recited in the claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

II. Regarding to the Appellant's arguments to claim 23 on anticipation by Takagi. Appellant states that "Takagi does not disclose utilizing the number of times a device has been authenticated (or "seed value") in his authentication method. Thus, Takagi does not disclose the claimed subject matter of claim 23. The claimed "**seed value**" is taught in the prior art. Since the term "seed value" is not described in the claim, Examiner interprets seed value as an ordinary value or data that store in a device. Takagi teaches in Figure 5, the initial state, **a same value I is stored in the first, second and third registers 205, 208 and 212**. For the I, a random number shared confidentially by the first and second communication devices (column 11, lines 41-44). Initially, when the transaction IC card 150 is inserted in the card terminal 100 which is equipped with the confirmation IC card 110, the first random number generation means 111 in the confirmation IC card 110 generates random number data R.sub.0, and the first encryption means 112 encrypts the random number data R.sub.0 provided by the first random number generation means 111 by using the first encryption key KE.sub.1 which is stored in advance in the confirmation IC card 110, and sends it to the transaction IC card 150 (column 9, lines 33-42 of Takagi). Thus, Takagi teaches the claimed "seed value". In addition, Appellant has argued such seed value may correspond to the number of times a device (such as the destination or source) has been authenticated (see Appellant's Appeal Brief, page 8, lines 23-25). This

clarification/limitation is not addressed in the claim. In fact, appellant is trying to equate the seed value as being the same as **number of times the device has been authenticated**. It is believed that the seed value is irrelevant to the **number of times the device has been authenticated**. Further explanation and/or clarification is needed from Appellant to equate these two terms/phrases. In response to appellant's argument that the references fail to show certain features of appellant's invention, it is noted that the features upon which appellant relies (i.e., **such seed value may correspond to the number of times a device (such as the destination or source) has been authenticated**) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

III. Regarding to the Appellant's arguments to claim 1 that Takagi fails to disclose storing information (such as identifiers) that is utilized when the devices are reconnected at a subsequent time (see Appellant's Appeal Brief, page 10, last paragraph). First of all, the phrase "**a subsequent time**" is not recited in the claim. In response to appellant's argument that the references fail to show certain features of appellant's invention, it is noted that the features upon which appellant relies (i.e., **a subsequent time**) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

Secondly, the second identifier **which was previously stored** in the first device and the first identifier **which was previously stored** in the second device. The phrase "**which was previously stored**" again is not recited in the claim. In response to appellant's argument that the references fail to show certain features of appellant's invention, it is noted that the features upon which appellant relies (i.e., **a subsequent time**) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

Thirdly, Takagi teaches the first processing means which has been granted the information exchange sends the transmission data to the first

Art Unit: 2135

communication means, and the first communication means 1 uses the random number data provided by the random number generation means to encrypt the entered transmission data and sends it to the card terminal. The encrypted data received by the card terminal is entered to the second communication means, and the second communication means uses the random number data received from the IC card to decrypt the entered encrypted data and enters it to the second processing means, which is the second communication device (column 4, lines 11-23 of Takagi). In addition, Takagi further teaches the first communication device is provided (e.g. stored) with random number generation means and first encryption means, and the second communication device is provided (e.g. stored) with second encryption means, and therefore a random number flowing from the first communication device to the second communication device is encrypted by the first encryption means, and a random number flowing from the second communication device to the first communication device is encrypted by the second encryption means (column 4, lines 46-57 of Takagi). Furthermore, Takagi teaches the procedure of creating the identifier described above in connection with Figure 6 is completely identical to the procedure of data encryption shown in Figure 5, and it is possible to have the identifier creation process and data encryption process concurrently. Namely, the output of the encryption processes 223-226 in Figure 6 is sent to the second device 202 as an output (encrypted output of transmission data) of the encryption means 204. Specifically, the output of the encryption process 226, i.e., the identifier 231, in Figure 6 is the output of the encryption means 204 for the fixed pattern (P) 215 in Figure 5, and it is stored in the second register 208. Next, the second device 202 uses the second encryption means 211 which performs the same operation as of the first encryption means 204, third register 212 and third exclusive-OR operation means 213 to create comparison data in the same procedure as that of the first device 201 for creating the identifier 231. The comparison data is stored in the third register 212. Finally, the second device 202 uses the comparison means 214 to compare the identifier 231 stored in the second register 208 with the comparison data stored in the third register 212 thereby to verify whether



or not the communication data has been tampered (column 12, line 59 through column 13, line 40 of Takagi). Thus, Takagi teaches the claimed subject matter of claim 1.

It is therefore shown that the components disclosed by Takagi constitute the claimed “the first device storing the second identifier and the second device storing the first identifier; when the first and second devices are disconnected and reconnected, the first device sending the first identifier to the second device and the second device sending the second identifier to the first device during the first reconnection, and each device comparing the received identifier against the stored identifier and sending additional information to the other device depending upon the result of the comparison.” It is so well known in the art that without information storing in the IC cards, data cannot be exchanged at all between the two devices as shown in Figure 1 of Takagi. Besides the disconnection and reconnection between the first and second devices discloses in Takagi’s system where in the card itself can be first device and the card reader can be second device as show in Figure 1. Such an application would have been obvious because Takagi teaches applicability to insert the first device (i.e., IC card) in the card terminal, which is the second device, and because the execution of inserting (e.g., connecting or re-connecting), un-inserting (e.g., disconnecting), and re-inserting (e.g., re-connecting again) the IC card is well known.

IV. Regarding to the Appellant’s arguments to claim 17 that Takagi does not disclose an increment counter. In an attempt to cure this defect, the Examiner relies on the incrementor 302 of Nakagawa. First of all, the claimed “**value representing the number of times the system has taken an action**” is taught in the prior art. The appellant is not very clear in describing this limitation in the claim; specially, the phrase “**taken an action**”. Examiner interprets the terminology as an act of doing any task, i.e., an act for storing, an act for retrieving.

Takagi teaches the comparison logic using registers and XOR for comparing the two data and/or information, as shown in Figure 7, wherein this comparison logic is obvious to derive the counter for how many times the data or information is storing to be compared. The missing counter in Takagi is disclosed by Nakagawa. Nakagawa teaches in Figure 1, an example of a conventional program

execution control device (hereinafter referred to as a "program control unit") for controlling a program execution order in a microprocessor or the like. **With reference to Figure 1, a conventional program control unit includes a program counter (PC) 300, an instruction memory 32, an instruction decoder 34, an incrementer 302 and a selector 304. Instruction memory 32 stores instructions of a program in the order of program addresses. Program addresses are ordinarily set to be incremented one by one.** In instruction memory 32, the program addresses are arranged in a continuous memory space whose addresses are incremented one by one. Instruction memory 32 is reading an instruction word 38 (of m-bit) from an applied n-bit address 310 and applying the word to instruction decoder 34 (column 1, lines 22-36). Nakagawa further discloses with reference to Figure 4, the program control unit of the present embodiment includes an instruction memory 32, an instruction decoder and a pseudo-random number program counter 30. Instruction memory 32 and instruction decoder 34 are the same as those of the conventional device shown in Figure 1, except that a program stored in instruction memory 32 is different from that of Figure 1. The program will be detailed later. An output 38 of instruction memory 32, a control signal 40, a select signal 42 and a jump address 44 output from instruction decoder 34 are also the same as those shown in FIG. 1 and no detailed description thereof will be repeated here (column 7, lines 12-24 of Nakagawa).

In response to appellant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988) and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, the combination of teachings between Takagi and Nakagawa is sufficient. Takagi teaches the claimed subject matter, but is silent about the use of the increment counter within Takagi's data storage area. This limitation is met by Nakagawa on column 1,

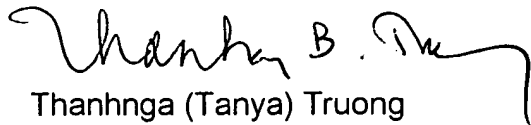
lines 22-36 and column 7, lines 12-24. Thus, the combination of teachings between Takagi and Nakagawa teaches the claimed subject matter of claim 17.

V. Regarding to the Appellant's arguments to claim 32 that neither Takagi nor Nakagawa as applied by the Examiner discloses the claimed subject matter: a first device having an identifier and pseudo-random number generator; a second device; and whereby upon the connection of the first device to the second device, the first device sends a value based on the output of the pseudo-random number generator and identifier, the second device receives the value, compares the received value with a prestored value, and depending on the results of the comparison, sends or receives information to or from the first device. First of all, the claimed **"depending on the results of the comparison, sends or receives information to or from the first device"** is taught in the prior art. Takagi teaches referring to Figure 9, a card terminal 400 comprises a random number generation means 401 which generates a random number R, a first computation means 402 which performs a functional computation F.sub.1 for first confidential data K.sub.1 and the random number R provided by said random number generation means 401, comparison means 403 which compares data provided by said first computation means 402 and data entered from an IC card 450, first processing means 406 which performs such data processing as data input/output, storing and operation, first encryption means 404 which encrypts the data sent out from said first processing means by using a first encryption key KE.sub.1, second decryption means 405 which decrypts encrypted data entered from the IC card 450 by using a second decryption key KD.sub.2 (column 1, lines 17-31 of Takagi). It is obvious for the Takagi's comparison 403 is used for comparing data transmitting or receiving from the first computation device. Thus, Takagi teaches the claimed subject matter in claim 32.



#### **(11) Related Proceeding(s) Appendix**

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

Respectfully submitted,



Thanhnga (Tanya) Truong  
March 01, 2006

Conferees  
Kim Vu   
Hosuk Song 



KIM VU  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100

LERNER, DAVID, LITTENBERG, KRUMHOLZ & MENTLIK, LLP  
600 South Avenue West  
Westfield, New Jersey 07090